RSAC | 2025 Conference

Many Voices.
One Community.

SESSION ID: PDP-R03

Data-Centric Security: Why Granular is Great

Will Ackerly

Co-Founder and Chief Architect
Virtru

Dana Morris

SVP, Product and Engineering
Virtru

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The Past: Perimeter Centric Security

* Trusted Data Format (TDF) invented at NSA by Virtru co-founder Will Ackerly

The Hard Truth: The Walls Are Crumbling

Findings:
10,626 data breaches; 100% YoY increase

Reality:
Legacy perimeter-centric security creates friction for people trying to share sensitive information

Today's Data Security Imperatives

Defense

Protect what we have
from being **lost** or **stolen**
(minimize risk)

Offense

Share what we must without
sacrificing **control** or **agility**
(drive value)

Security Perimeters: ‘Shift Happens’

Defense

Perimeter-Based

Offense

Data Centric Based

RSAC | 2025 Conference

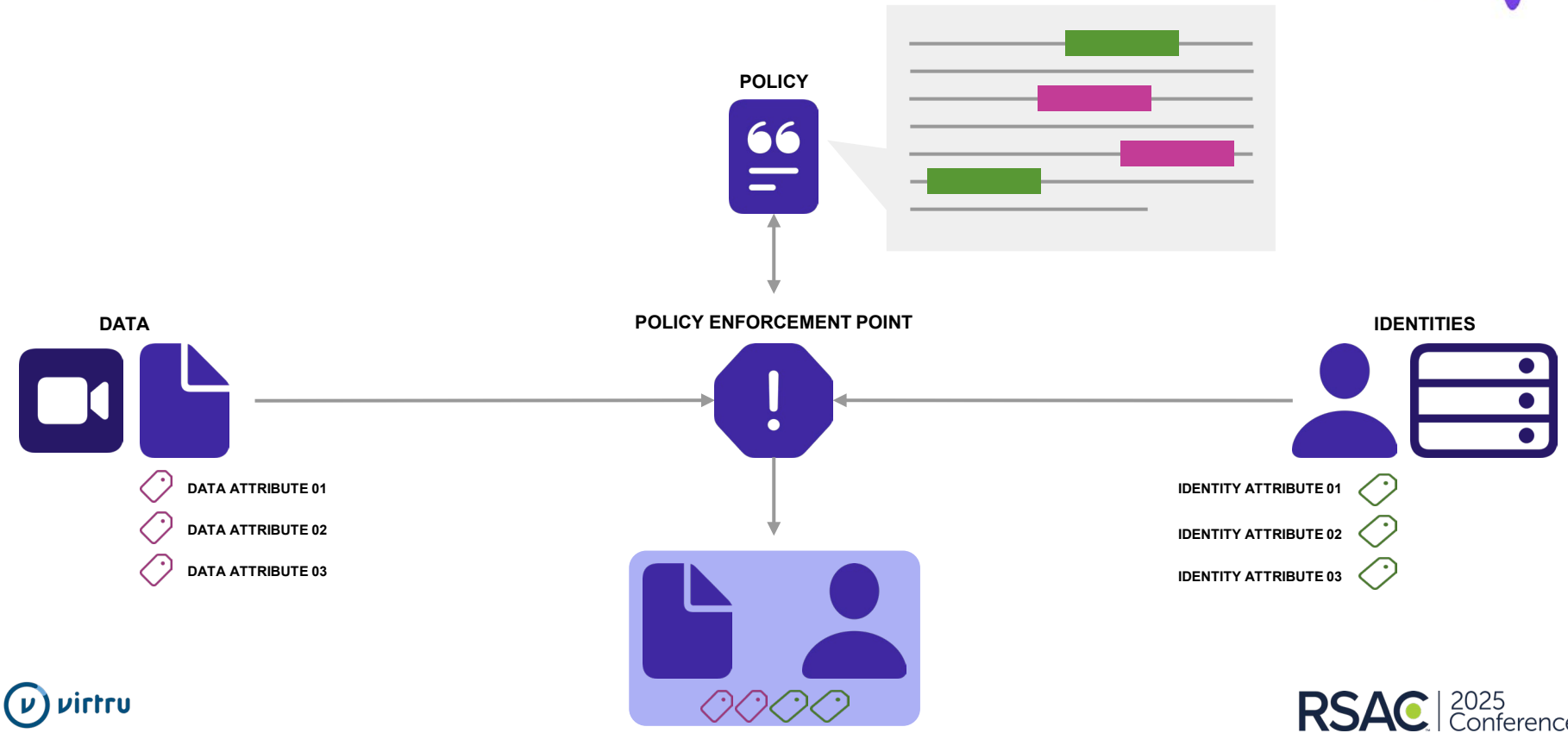
Attribute Based Access Control

What is Attribute Based Access Control (ABAC)?

Attribute-Based Access Control (ABAC) is an **authorization model** that determines access to information based on **characteristics** of the **data** and **identities** involved.

Its purpose is to enable the definition of more dynamic access control rules, ensuring that users without the "approved" characteristics, as specified by an organization's security policies, are prevented from performing unauthorized actions.

Attribute-Based Access Control (ABAC)



The Building Blocks of ABAC

1. Attributes
2. Entitlements
3. Policies

Attributes are the foundational elements that drive the access control decisions in ABAC. They represent the **characteristics or properties** of the entities involved in an access request, including the **identity** (e.g., user or device), the **data**, and the environment (e.g., time, location or network).

The Building Blocks of ABAC

1. Attributes
2. Entitlements
3. Policies

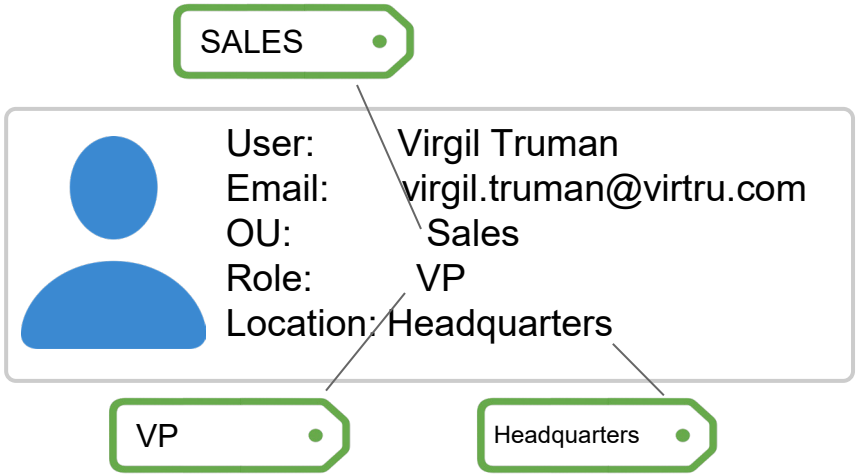
Entitlements represent the **permissions or actions** an **identity** (e.g., a user or device) can perform on a particular **resource** (.e.g., file or document). These entitlements are dynamically granted or denied based on evaluating policies that consider various attributes of the identity, data, and environment.

The Building Blocks of ABAC

1. Attributes
2. Entitlements
3. Policies

Policies are the core components that **define the rules** for granting or denying **access to resources** based on various attributes. These policies bridge the gap between attributes and entitlements by specifying the **conditions** under which certain entitlements should be granted or denied.

Identity Attributes



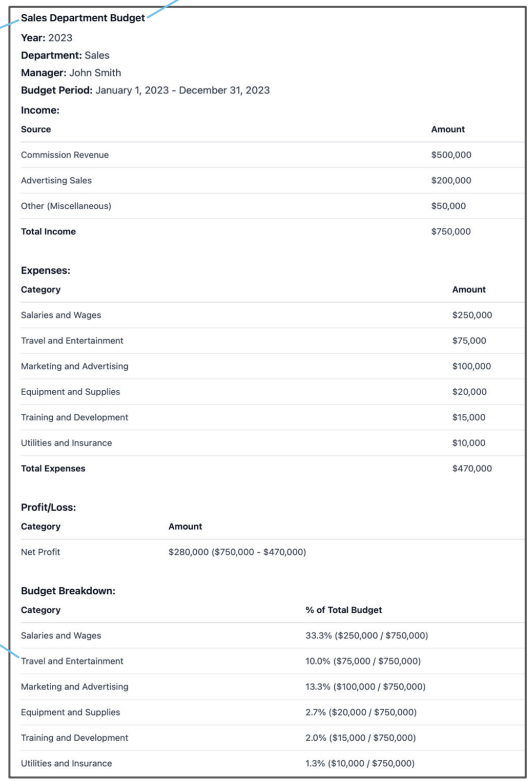
NAME	VALUE
OU	Sales
Role	VP
Location	Headquarters

Data Attributes

BUDGET

SALES

LIMITED



Sales Department Budget

Year: 2023
Department: Sales
Manager: John Smith
Budget Period: January 1, 2023 - December 31, 2023

Income:

Source	Amount
Commission Revenue	$500,000
Advertising Sales	$200,000
Other (Miscellaneous)	$50,000
Total Income	$750,000

Expenses:

Category	Amount
Salaries and Wages	$250,000
Travel and Entertainment	$75,000
Marketing and Advertising	$100,000
Equipment and Supplies	$20,000
Training and Development	$15,000
Utilities and Insurance	$10,000
Total Expenses	$470,000

Profit/Loss:

Category	Amount
Net Profit	$280,000 ($750,000 - $470,000)

Budget Breakdown:

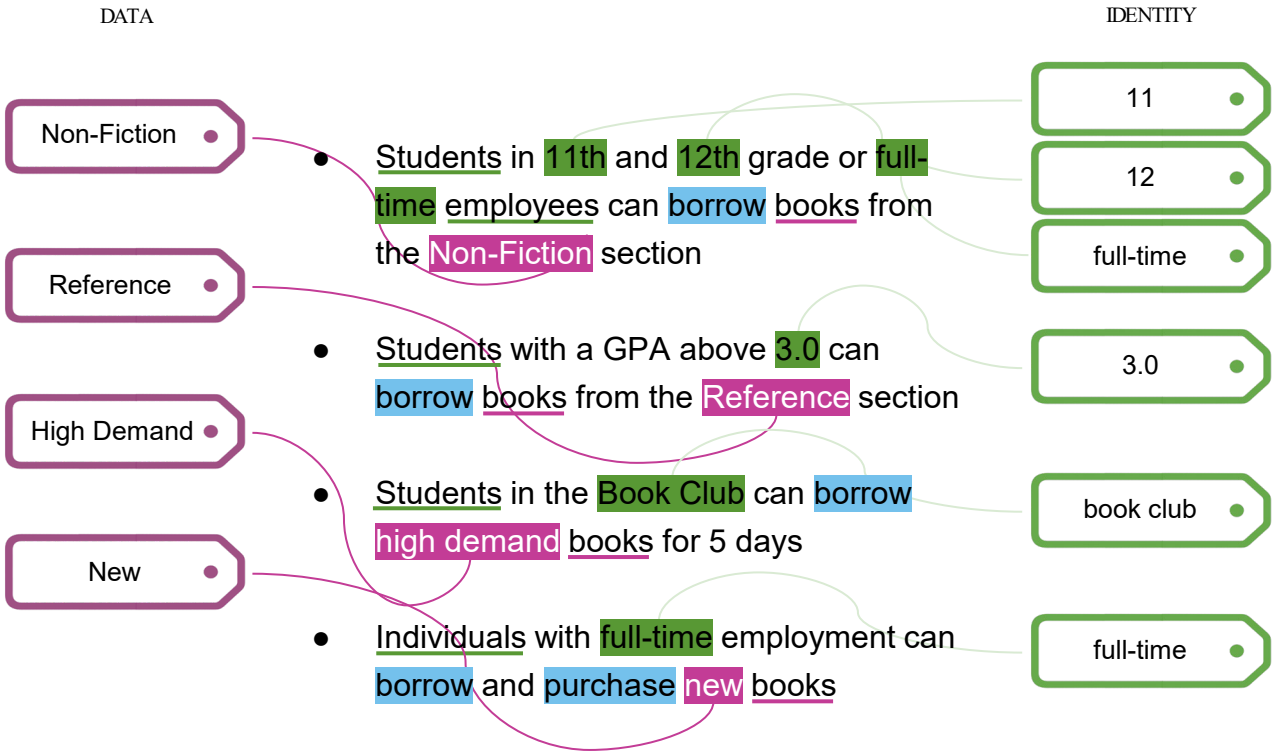
Category	% of Total Budget
Salaries and Wages	33.3% ($250,000 / $750,000)
Travel and Entertainment	10.0% ($75,000 / $750,000)
Marketing and Advertising	13.3% ($100,000 / $750,000)
Equipment and Supplies	2.7% ($20,000 / $750,000)
Training and Development	2.0% ($15,000 / $750,000)
Utilities and Insurance	1.3% ($10,000 / $750,000)

NAME	VALUE
Dept	Sales
DocType	Budget
Sensitivity	Limited

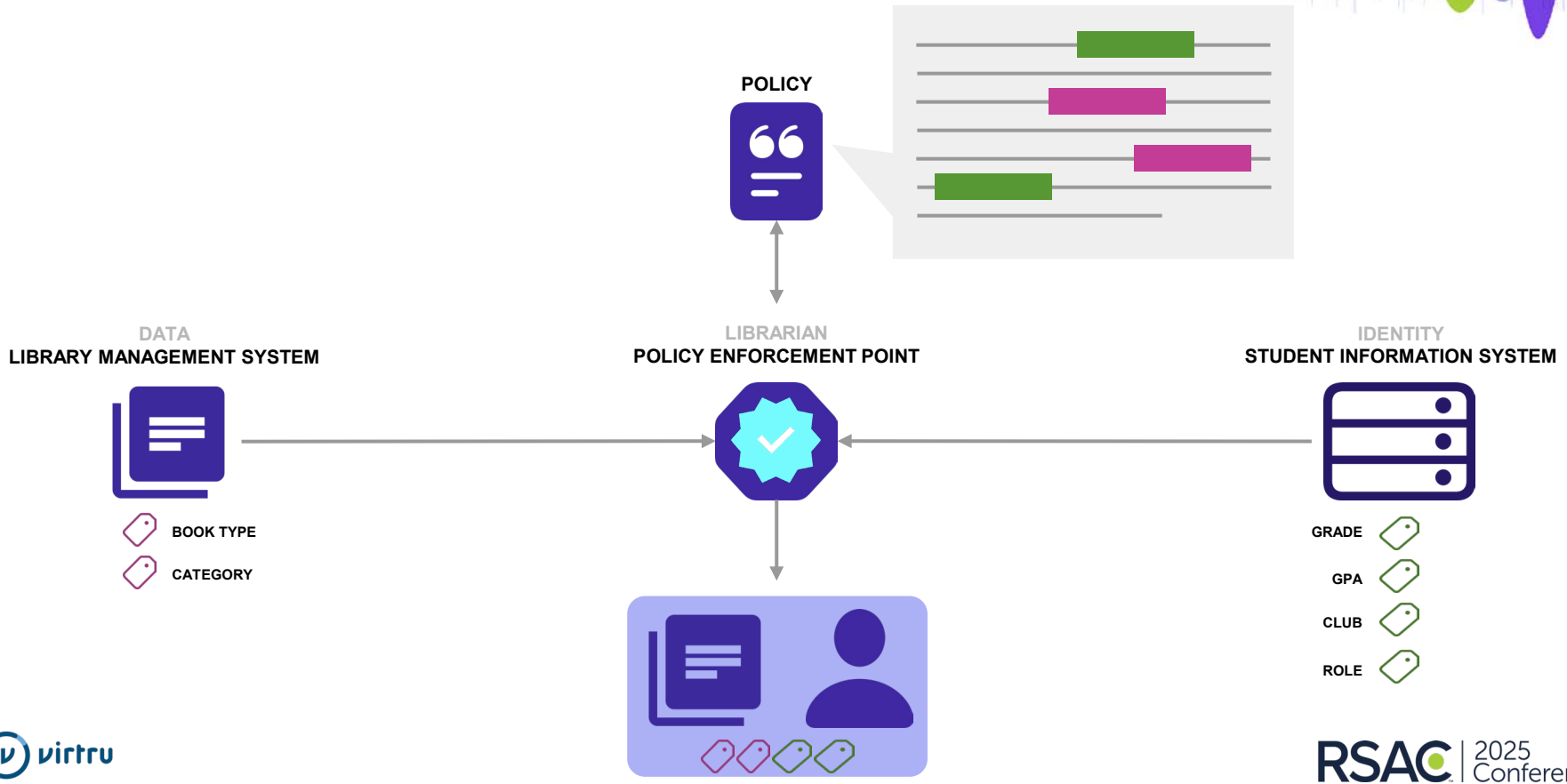
Example: School Library Book Policies

- Students in 11th and 12th grade or full-time employees can borrow books from the Non-Fiction section
- Students with a GPA above 3.0 can borrow books from the Reference section
- Students in the Book Club can borrow high demand books for 5 days
- Individuals with full-time employment can borrow and purchase new books

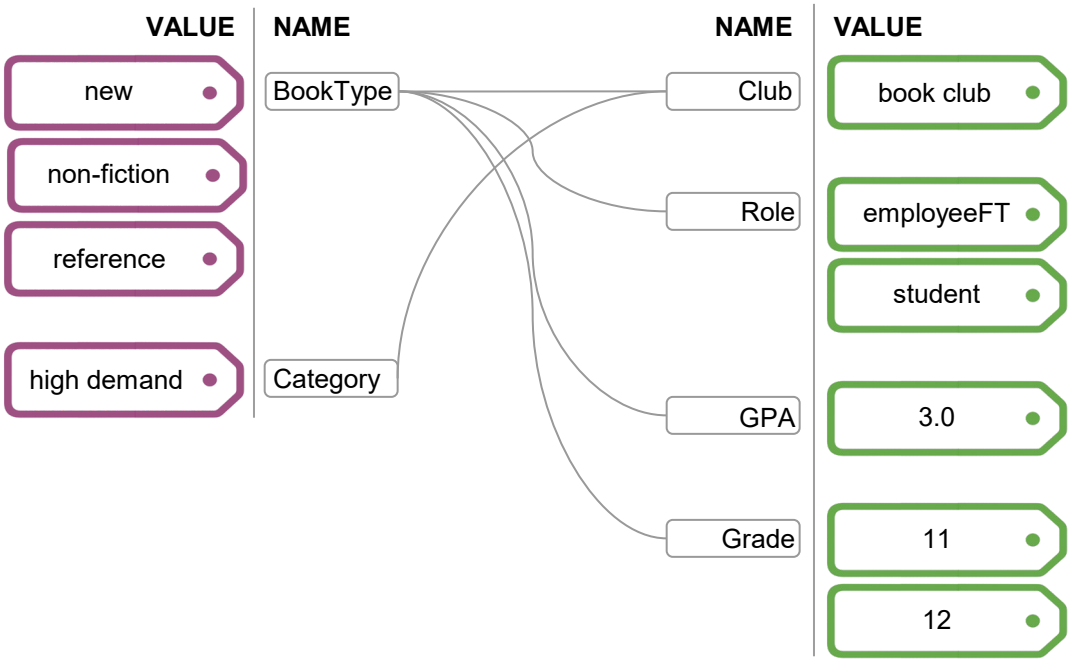
Example: School Library Book Policies – Attributes



Example: Attributes & Enforcement



Example: School Library Book Policies – Attribute Mapping



RSAC | 2025 Conference

Trusted Data Format

Trusted Data Format

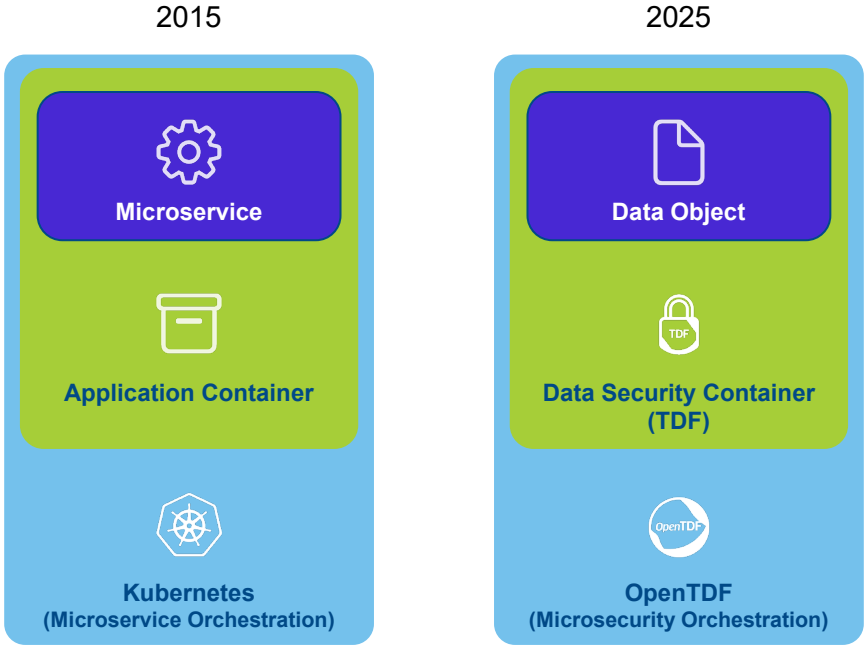
- Open, interoperable data encoding format for implementing data-centric security
- Standard to define and enforce object-level policy that keeps sensitive data protected and under the owner's control, wherever it goes
- Extensible for your organization's needs

Why TDF?

Securely share data outside your organization and boundary

History is Repeating Itself

Apps:
monolithic to microservices

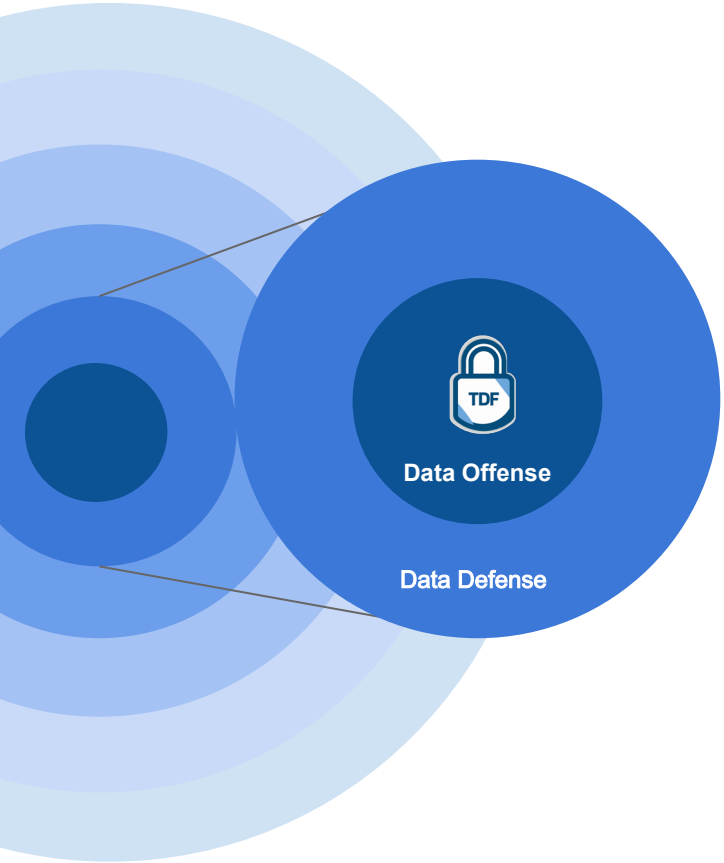


Security:
perimeter to data centric

Data Centric Security: Where TDF Fits

- Identities
- Endpoints & Devices
- Networks
- Apps
- Prevent Data Loss
- Promote Data Sharing

Offense vs Defense



- Data pillar of Zero Trust
- Promote intentional sharing of data
- Granular policy and access controls
- Adjacent and complementary to other security tools

What can TDF enable?

01 Strong data control

02 Attribute-based access control (ABAC)

03 Strong encryption

04 Policy Binding

05 End–to-end auditability

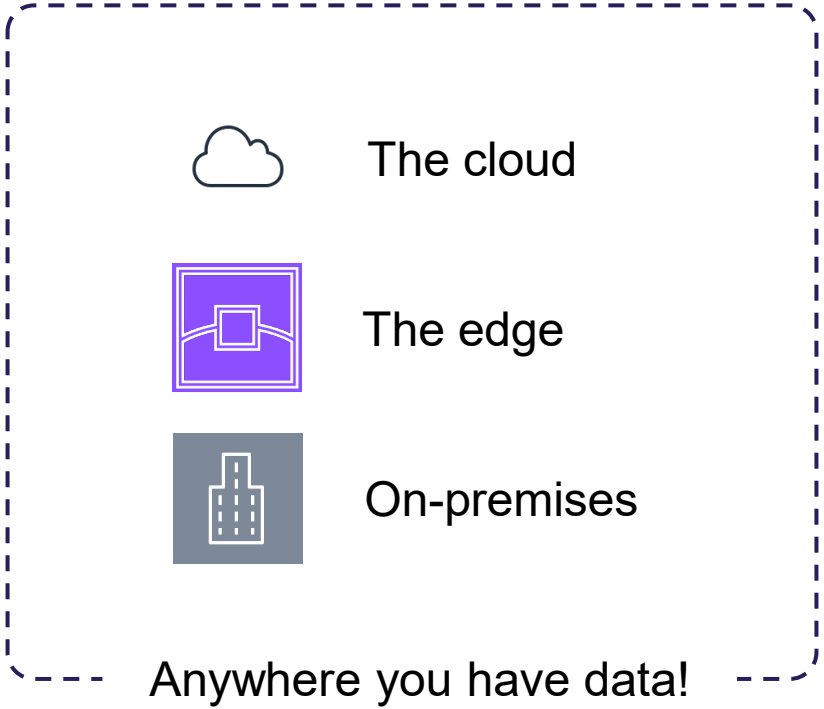
06 Streaming and support for large files

07 Offline create

08 Key server federation

Where and how can we use TDF?

- General data sharing
- Disconnected operations
- Generative AI



OpenTDF

OpenTDF is an open-source system for implementing data-centric security; it provides the basic services required to enable the definition, application, and enforcement of attribute-based policies using the **Trusted Data Format**

Services
Core services that enables you to build data-centric security into your applications

Specification
The TDF schema and protocol specification, fully compliant with the ZTDF

CLI
A command line experience for managing an OpenTDF platform instance

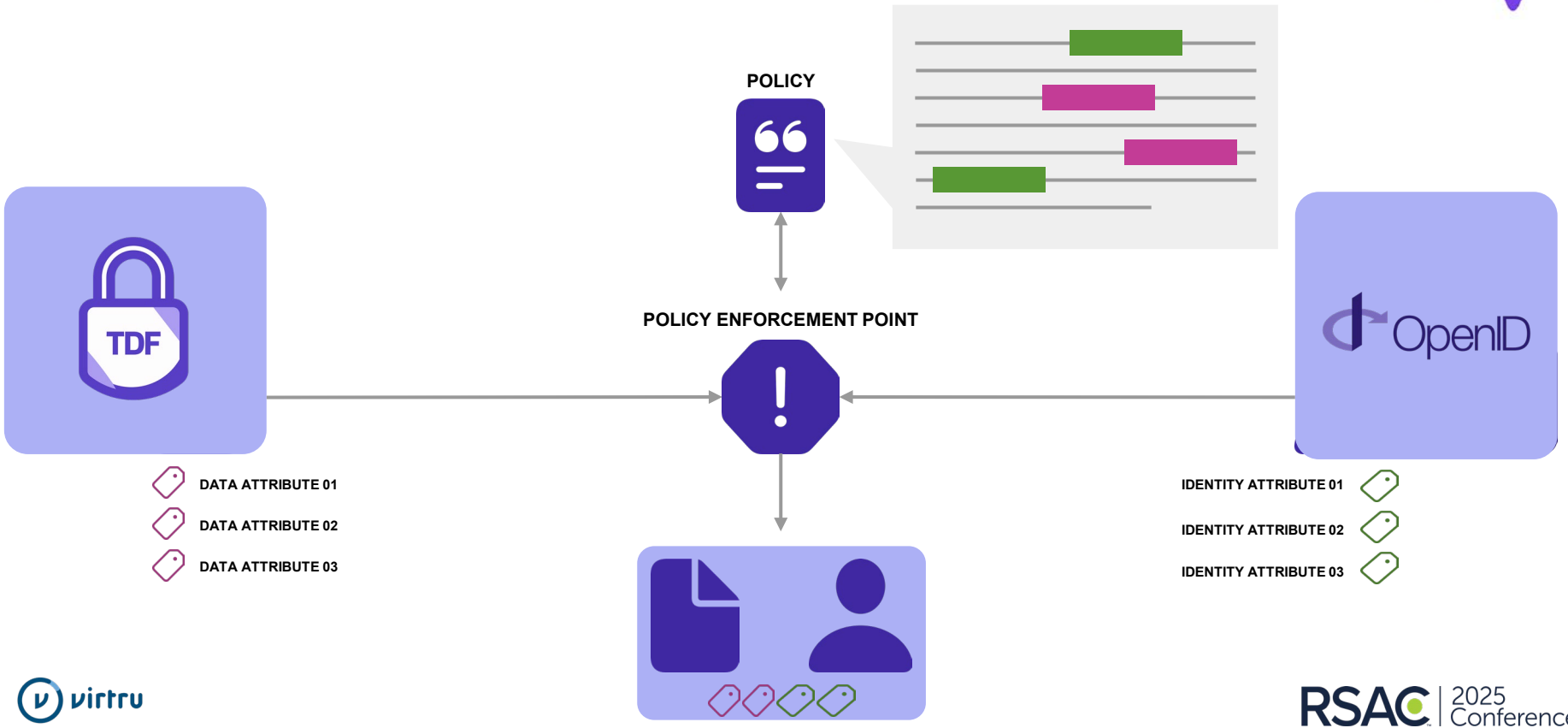
https://github.com/opentdf

RSAC | 2025 Conference

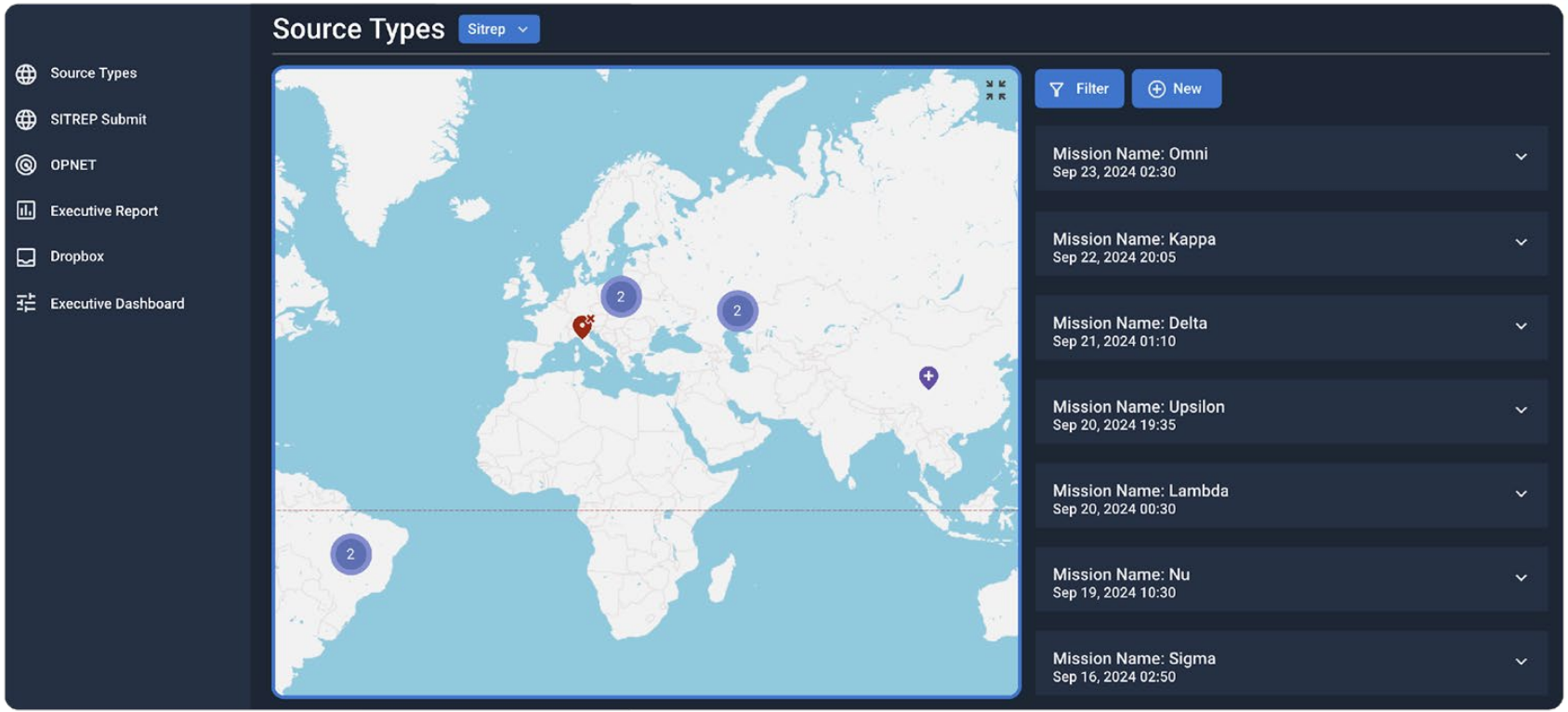
TDF + ABAC

Granular Security

Attribute-Based Access Control (ABAC)



Common Operating Picture Example



RSAC 2025 Conference

Common Operating Picture Demo

RSAC | 2025 Conference

Wrapping Up

Summary

TDF + ABAC: Benefits

- Protects at Data Level – Policy-wrapped data with attribute-based access
- Adapts Dynamically – Flexible controls based on changing conditions
- Reduces Risk – Limits access to only what's necessary, when necessary
- Ensures Compliance – Meets regulatory requirements through precise controls

Apply What You Learned Today

- Next Week
  - Learn about Attribute Based Access Control
  - Review Data Centric Security resources
  - Check if your organization classifies data
- Next 3 Months
  - Assess data discovery and classification practices
  - Review identity attributes and requirements
  - Identify opportunities for controlled data sharing
  - Map data flows for security improvements
- Consider Options
  - Explore commercial and open source solutions
  - Run a proof-of-concept test

RSAC | 2025 Conference

Many Voices.
One Community.

Thank You

For More Information:

opentdf.io